**IT Applications Unit 3, AOS 1, Online Communities**

1. Complete the following, from pgs, 32: **Network security**

**Networks are classified according to below and we will study the following:**

1. Network Categories: LAN, WAN
2. Network Architecture, client-server; peer-to-peer; internet peer-to-peer; intranet
3. Network communication standards
4. Network hardware and software
5. Transmission media
6. **Network security**
7. What types of physical security measures can be put in place?

**Usernames and passwords**

1. Recommend a password strategy that an organisation could use to avoid unauthorised access to the network.

* Be at least eight digits long
* Including non-alphabetical character
* Not be easily guessed
* Be changed every month

**Firewall**

1. Describe the nature of a firewall.

A firewall is a server and software combination that filters the information coming through an internet connection into an originations internal network.

1. What are the main purposes of firewalls and how are these purposes achieved?

Any packet of data that is flagged by the filters as unwanted is not allowed though.

1. Why do firewalls use 2 separate NICs?

One is connected to the internal network and the other to the outside world.

**Malware protection**

1. What is malware and what strategies are used to protect against this type of software?

Malware is malicious software and to protect agents them you need to run protection software.

**Encryption**

1. What is encryption?

Encryption is the process of translating data into secret code that can only be read by authorised users.

1. Describe the nature of WPA or WPA2.

WPA or WPA2 is a protocol for used by wireless LANs. It provides security by encrypting data sent over radio waves.

1. What is encrypted data known as?

Ciphertext

**Secure Websites**

1. Describe the secure protocol to allow secure financial transactions across the internet.

Hypertext transfer protocol security is the secure protocol between a client’s web browser and the web server, to ensure that a secure connection is established and maintained.

1. What is digital identification certificate technology based on?

It is based on a trusted certificate authority such as VeriSign Incorporated

1. Describe the nature of Secure sockets layer (SSL) protocol.

It’s a cryptographic protocol that provides secure connection on the internet.

**Physical design of networks**

1. What is the role of a network diagram?

It’s a schematic method of showing the physical devices and communications lines present in a network.